

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-076360

(43)Date of publication of application : 14.03.2000

(51)Int.Cl.

G06F 19/00  
H04N 1/387  
// G06F 17/30  
G06T 7/00  
G09C 5/00

(21)Application number : 10-244721

(71)Applicant : HITACHI LTD

(22)Date of filing : 31.08.1998

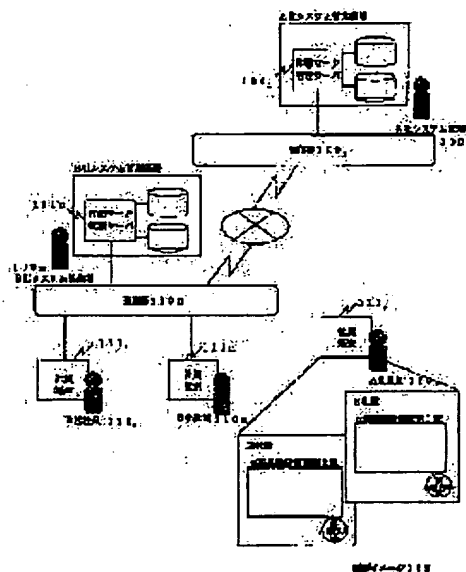
(72)Inventor : KAWANISHI YASUNORI  
TOYOSHIMA HISASHI  
NAGAI YASUHIKO

(54) METHOD AND DEVICE FOR DOCUMENT MANAGEMENT AND STORAGE MEDIUM STORED WITH DOCUMENT MANAGING PROGRAM

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide an electronic seal duplication management system which can use a free seal impression design, confirm the original and its copy, and allow a user to manage the original and copy synchronously by dynamically varying the validity and originality of data as to the transfer of data through a network.

**SOLUTION:** At a request from an employee 1101, a system administrator 1001 embeds seal mark information ciphered with a cipher key managed by a seal mark administrating device 1011 in the mark of a seal impression design that the employee 1101 has generated and sent. An open key needed for the deciphering of it is attached to the seal mark or distributed previously to an employee 1111 in the company and a relative system administrator 100n outside the company. On a reception side, it can be confirmed with the previously distributed open key or open key attached to the seal mark that the seal mark information is embedded in the seal mark, so the originality and validity of a document certificate can be controlled and confirmed through the network.



## LEGAL STATUS

[Date of request for examination] 13.02.2002

[Date of sending the examiner's decision of rejection] 08.06.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-76360

(P2000-76360A)

(43)公開日 平成12年3月14日(2000.3.14)

(51)Int.Cl.	識別記号	F I	キーワード(参考)
G 0 6 F 19/00		G 0 6 F 15/22	N 5 B 0 4 3
H 0 4 N 1/387		H 0 4 N 1/387	5 B 0 7 5
G 0 6 P 17/30		G 0 9 C 5/00	5 C 0 7 6
G 0 6 T 7/00		G 0 6 F 15/40	3 7 0 B 5 J 1 0 4
G 0 9 C 5/00		15/62	4 5 5 9 A 0 0 1

審査請求 未請求 請求項の数 7 O L (全 17 頁) 最終頁に続く

(21)出願番号 特願平10-244721

(22)出願日 平成10年8月31日(1998.8.31)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 川西 康則

神奈川県横浜市都筑区加賀原二丁目2番

株式会社日立製作所システム開発本部内

(72)発明者 豊島 久

東京都江東区新砂一丁目6番27号 株式会社

日立製作所公共情報事業部内

(74)代理人 100088504

弁理士 小川 勝男

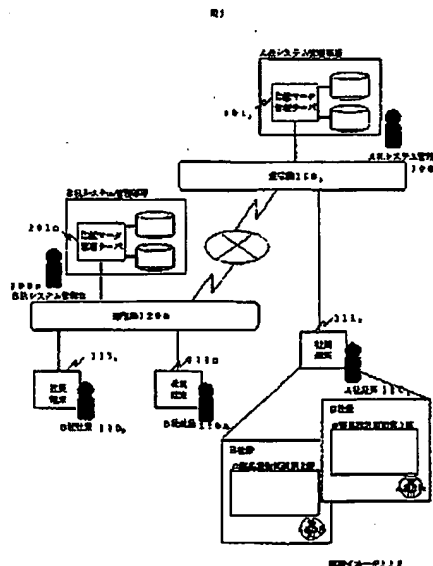
最終頁に続く

(54)【発明の名称】 文書管理方法および装置並びに文書管理プログラムを格納した記憶媒体

(57)【要約】

【課題】データのネットワーク上でのやり取りにおいて、自由な印影デザインを使用でき、原本と複製とを確認でき、データの有効性と原本性を利用者が動的に変化させて、かつ原本と複製とが同額をとって管理する事を可能とする、電子印鑑複製管理システムを提供する。

【解決手段】システム管理者100が、社員110の要求に応じて、印鑑マーク管理装置101が管理する暗号鍵で暗号化した印鑑マーク情報を、社員110が作成・送信した印影デザインのマークに埋め込む。この復号化に必要な公開鍵は印鑑マークに添付するか、予め社内の社員端末111に関連する社外のシステム管理者100nに配布する。受信した側は、予め配布された公開鍵、または印鑑マークに添付された公開鍵で印鑑マークに埋め込まれたを確認することができるので、ネットワーク上で文書認証及び原本性や有効性の制御及び確認を行うことができる。



特開2000-76360

(2)

1

## 【特許請求の範囲】

【請求項1】 少なくとも1つの端末と、前記端末で使用される印影または署名（サイン）を表すイメージデータ（以下これをマークと称する）を管理する少なくとも1つの管理装置とが通信網を介して相互に接続されており、

前記マーク管理装置は、前記端末からマークの登録あるいは変更要求を受けた場合に、データの原本性及び原本からの複製であること（以下これを複製性と称する）を確認するために必要な情報を登録及び管理する手段を備え、

前記端末は、データの原本性及び有効性の確認を行うために必要な情報をマークに埋め込む手段と、該マークをデータに押印できる手段と、データの有効性を制御する手段と、データの原本性及び複製性のいずれか一方または双方を確認できる手段を備えることを特徴とする文書管理装置。

【請求項2】 請求項1に記載の文書管理装置において、マーク管理装置で、データ原本に押印された原本マークと、データ複製に押印された複製マークとを階層的に管理する手段を備えることを特徴とする文書管理装置。

【請求項3】 請求項1に記載の文書管理装置において、画像データであるイメージデータを2つ以上のブロックに分け、データの原本性及び有効性を確認するために必要な情報と文書が改ざんされていないこと（以下、単に文書認証と称することもある）を確認するために必要な情報を該イメージデータの異なるブロックに加えて、データの原本性及び有効性のいずれか一方または双方を確認できる手段を備えた視認性のある印影マークを生成することを特徴とする文書管理装置。

【請求項4】 請求項1に記載の文書管理装置において、可視透かしと不可視透かしを併用して、データの原本性及び有効性を確認する手段を備えた視認性のある印影マークを生成することを特徴とする文書管理装置。

【請求項5】 請求項1に記載の文書管理装置において、マーク管理装置でデータの原本性及び有効性、押印や複製に関する情報の管理を行うために必要な情報を暗号化したものをマークに埋め込み、その復号化に必要な公開鍵を印影マークに添付することで、イントラネットに限らず、ネットワーク上で原本性及び有効性の確認及び、複製可否の判断を行うことを特徴とする文書管理装置。

【請求項6】 請求項1に記載の電子印影複製管理システムにおいて、端末で、マーク付きのデータを複製でき、原本マークから複製マークへ情報を継承することを特徴とする、電子印影複製管理システム

【請求項7】 請求項1に記載の文書管理装置において、端末で、データの原本性及び有効性の確認を行うために必要な情報をマークに埋め込む機能と、データの原本性及び有効性のいずれか一方または双方を確認する機能を備えたインターフェイスを特徴とする文書管理装置。

2

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、文書の原本性及び有効性を電子印影により認証する方法および装置並びに、その方法を実現した文書管理プログラムを格納した記憶媒体に関するものである。

【0002】

【従来の技術】 ネットワーク上で流通するデータが増加しつつある現在、データの信頼性をネットワーク上で確認できる技術が重要になってきている。

【0003】 また、グループウェアの普及に伴って、データを承認する際に、承認者が控えとして承認後のデータを複製したり、承認されたデータをネットワーク上で閲覧する際に、閲覧中の閲覧者が、承認されたデータを個人用として複製する機会が増加している。

【0004】 また、ネットワーク上での商取引の増加に伴って、決済の際に支払いを証明するために、データ上でも領収書の役割が必要になっている。従来の紙で行われてきたカーボンコピーのように、特定の数だけ複製が必要で、かつ改ざんが不可能な手段がデータ上でも必要となっている。

【0005】 データの途中改ざんの確認については、インターネットを利用したECで、クレジット決済を安全に行うために用いられるSETでは、デジタル署名によるカード所有者の認証を行っている。デジタル署名は、通常伝送したい情報を圧縮した圧縮文を送り手の暗号鍵で暗号化した暗号文であり、送り手の復号鍵（公開鍵）で元の圧縮文に復号化できる。つまり、受け手は受け取ったメッセージから作った圧縮文と受けとったデジタル署名から復号化した圧縮文とを比較することで、メッセージが改ざんされていないかの確認、つまり文書認証ができる。

【0006】 一方、印影や署名が一般的に持つ意味合いは、原本性の確認と文書認証を合わせ持つと考えられる。これらを解決する技術として、特開平10-11509（以下、従来技術1と呼ぶ）に開示されているような印影やサインなどを文書に付加し、その形などを文書の複製で変形させ、その認証を可能にすることにより文書の改ざんを防止する方式も開発されている。また、特開平6-176036（以下、従来技術2と呼ぶ）に開示されているように、IDカードと複写機を用いて現行文書の原本性及び複製性を確認する方式も開発されている。

【0007】

【発明が解決しようとする課題】 デジタル署名は、文書認証とデータの有効性を表す両方の機能を有するともいえるが、データの受け手はそのデータを見ただけでは、情報の正当性及び有効性の確認をすることはできない。現実社会では真印の押印のように、見て確認することにより安心感を待たせることができるが、デジタル署名はこ

(3)

特開2000-76360

のような視認性を待たない。

【0008】一方、従来の電子印鑑システムは、目で見えて確認できる印影を用いるが、印影自体は単なるデザインであって、電子印鑑付きのデータを複製すると、原本と複製の見分けが困難であった。例えば、戸籍票や登記簿などの、原本と複製（抄本）のそれぞれが意味を持ち、かつ印影による承認で価値を有する場合において、原本と複製とで同期をとって、有効性及び無効性を管理する必要がある。しかしながら、従来の複製可能な電子印鑑システムでは、データの原本と複製との間で同期をとって、有効性及び無効性を管理する事が不可能であった。

【0009】つまり、データの真正性と原本性の保証が必要でかつ、データを複製する場合や、複製するデータの数を限定する場合、複製の可否を利用者が任意に制限する場合に有効な手段が無かったといえる。

【0010】また、従来技術1においても、印影自体は単なるデザインデータであって、文書認証を行うためには、サーバ上の善悪となる印影と、文書の特徴量で変形させた印影とを比較する必要がある。つまり、特定のイントラネット内におけるオンラインでの文書認証はできるが、企業間のネットワーク、例えばエクストラネット等でのデータのやり取りにおいて、データの受け手が、表示されたデータ上で文書認証することはできなかった。また、表示されたデータ上で、その原本性や有効性を制限したり確認することができる機能を備えている電子印鑑システムはなかったといえる。

【0011】従来技術2では、複写機においてハードコピーの原本性と複製性をとを認証する手段を提供してはいるが、データの原本性と有効性とを確認することはできなかった。

【0012】本発明の目的は、視認性のある印影でデータの真正性を保証し、データの真正性を確認でき、かつ原本性と有効性を制御及び確認できる電子印鑑複製管理システムを提供することである。

【0013】

【課題を解決するための手段】上記の課題を解決するために、本発明では、少なくとも1つの端末と、その端末で使用される、視覚で確認できる性質や本人認証手段を備えたマークを管理する少なくとも1つのマーク管理装置とが通信網を介して相互に接続されており、前記マーク管理装置は、前記端末で使用するデータの原本性及び有効性確認に必要な情報を管理するマーク管理DBを備え、前記端末の要求に応じて、前記マーク管理装置で管理する暗号鍵で暗号化した原本性及び有効性を確認する情報をマークに埋め込み、公開鍵をマークに添付する又は端末や他のマーク管理装置に配布することで、マークに埋め込まれた情報を復元化する手段を備え、前記端末は、データの作成時に、前記マーク管理装置で生成した印鑑マーク押印や複製及び無効化の際に、原本性及び有

効性を確認するための情報を埋め込んだマークを入手する手段と、作成したデータが改ざんされていないことの確認（以下、単に文書認証と称する場合がある）情報を前記端末固有の秘密鍵で暗号化して該マークに埋め込み、公開鍵を添付することで、原本性及び有効性の確認と文書認証手段を備えたマークを生成し、データに押印する手段と、該マークを用いてデータの原本性及び有効性の確認と文書認証を行う手段を備えたシステムを構築することにより上記目的を達成することが可能となる。

【0014】

【発明の実施の形態】以下、図面を用いて本発明の実施形態の一例を説明する。ここでは、本発明の詳細を、企業イントラネット及び企業間ネットワークにおける電子印鑑複製管理システムの例を用いて説明する。なお、以下で説明する図面において同一の番号は同様の部品・要素を表すものとする。また、これにより本発明が限定されるものではない。

【0015】図1は、本発明の電子印鑑複製管理システムの概略構成を示したものである。本実施形態の電子印鑑複製管理システムは、印鑑マークを管理するシステム管理者1001～100n（以下、単にシステム管理者100とも称する）と、社員1101～110n（以下、単に社員110とも称する）が利用するシステムであって、図1に示すように、印鑑マーク管理装置1011（以下、単に印鑑マーク管理装置101とも称する）と、社員端末1111（以下、単に社員端末111とも称する）とが、企業イントラネットなどの通信網1201（以下、単に通信網120とも称する）を介して、互いに接続されて構成されている。これに、インターネットなどを經由して、他社の同様のシステム、あるいは端末が接続される。なお、ここでいう印鑑マークとは、視認性のある画像データであって、印鑑を押印された文書等のデータの原本性と有効性を確認でき、該データが改ざんされていないかの検証（以下、単に文書認証とも称する）、複製可否の確認、ができるという機能を持つ、印鑑やサイン等のイメージデザインの形状をとるマークを示すものとする。

【0016】印鑑マーク管理装置101は、システム管理者100が管理する、企業イントラネットや企業間のネットワーク取引で原本性及び有効性の制御及び確認や、文書認証を行う印鑑マーク管理用のサーバである。印鑑マーク管理装置101は、社員110の要求に応じて、原本性の確認に必要な情報を埋め込んだ印鑑マークを作成し、後述の印鑑マーク管理DB209及び印鑑押印管理DB210や印鑑複製管理DB211に登録する。

【0017】社員端末111は、社員110が利用する端末である。社員110は、社員端末111を使って、ビジネスに必要な文書等を作成したり、システム管理者100とデータのやり取りをしたりする。各目の印鑑マ

(4)

特開2000-76360

5

ークは、社員端末111などで管理する。所属等の情報変更時には、システム管理者100が印鑑マークの更新を行い、更新した印鑑マークを社員端末111に送信する。画面イメージ112は、印鑑マーク付きのデータを表示した時の画面イメージ例であり、データ(α部品設計図面第1版、同第2版)が作成されている図である。

【0018】図2は、印鑑マーク管理装置101のハードウェア構成を示したものである。

【0019】本実施形態の印鑑マーク管理装置101のハードウェア構成は、図2に示すように、表示装置201と、入力装置202と、通信網インタフェース203と、印鑑マーク管理DBインタフェース204と、印鑑マークログ管理DBインタフェース205と、記憶装置206と、中央処理装置(CPU)207と、一時記憶装置(メモリ)208とが、バス200によって互いに接続されて構成されている。また外部記憶装置として、印鑑マーク管理DB209と、印鑑マーク複製管理DB210が接続している。

【0020】表示装置201は、印鑑マーク管理装置101を使用するシステム管理者100にメッセージなどを表示するために用いられるものであり、CRTや液晶ディスプレイなどで構成されている。

【0021】入力装置202は、印鑑マーク管理装置101を使用するシステム管理者100がデータや命令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【0022】通信網インタフェース203は、通信網120を介して、社員端末111や他社の印鑑マーク管理装置101n等とデータのやり取りを行うためのインタフェースである。

【0023】印鑑マーク管理DBインタフェース204は、印鑑マーク押印管理DB209とデータのやり取りを行うためのインタフェースである。該印鑑マーク管理DB209は、社員ID、印鑑ID、印影などといったデータを対応づけて管理するものであり、例えば図4のようなものである。

【0024】また、該印鑑マーク管理プログラムは、印鑑マークをデータに押印する際に印鑑押印DB210とデータのやり取りを行う。該印鑑マーク押印管理DB210は、印鑑ID、通算NO、作成日時、複製可否フラグ、複製フラグ、無効フラグ、ファイル名、端末ID、データの特徴情報、といったデータを対応づけて管理するものであり、例えば図5のようなものである。

【0025】印鑑マーク複製管理インターフェース205は、印鑑マーク複製管理DB211とデータのやり取りを行うためのインタフェースである。印鑑マーク複製管理DB211は、社員端末111nで印鑑マークを複製する際のデータを対応づけて管理するものであり、上位印鑑通算NO、通算NO、複製年月日、複製社員ID、といったデータを対応づけて管理するものであり、

6

例えば図6のようなものである。

【0026】記憶装置206は、印鑑マーク管理装置101などで使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

【0027】CPU207は、印鑑マーク管理装置101を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【0028】メモリ208には、オペレーティングシステム208a(以下、単にOS208aとも称する)や印鑑マーク管理プログラム208b、印鑑マーク複製管理プログラム208cといった、CPU208が上記の処理をするために必要なプログラムなどが一時的に格納される。これらのプログラムはCD-ROMなどの記憶媒体に格納されて提供される。本システムのインストール時にハードディスクに格納し、起動時にメモリ208へ格納する。

【0029】ここで、OS208aは、印鑑マーク管理装置101全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【0030】真正性確認プログラム208dは特開平9-348860に開示されている印鑑マークが本物であるか否かを確認する方式と、印鑑マークが押印されているデータの真正性を確認する方式を前提として、印鑑マーク管理プログラム208bと印鑑マーク複製管理プログラム208cを実現する。

【0031】印鑑マーク管理プログラム208bは、社員端末111から押印要求があった場合に、印鑑マーク管理DB209を参照する処理、印鑑マーク押印管理DB210を登録/更新する処理、印鑑マークに特定の情報を埋め込む処理、要求元に印鑑マークを送信する処理を行う。ここでは、印鑑マーク管理DB209は既にデータが登録されているものとし、印鑑マーク管理DB209に対してデータを登録/更新する処理は、システム管理者100が行うものとするが、社員110が任意に行っても良い。

【0032】画像データの中に特定の情報を埋め込む技術は、「電子透かし」として知られている。「電子透かし」の技術については日経エレクトロニクス1997年683号の100ページから107ページに記載されている。人間の目では判別できないように情報を埋め込む不可視透かしと、人間の目にも見える形で情報を埋め込む可視透かしがあり、不可視透かしの場合埋め込む情報量に制限があるとされている。印鑑マークの場合、印鑑イメージが象徴する意味が分かる範囲、つまりそのマークが何を表すかが分かる範囲であれば、多少デザインを変更しても支障がないので、図7のように、可視透かしと不可視透かしを組み合わせ、ある程度多くの情報を埋め込むことができる。

(5)

特開2000-76360

7

【0033】また、該印鑑マーク管理プログラムは社員端末111から印鑑マーク無効化処理要求があった場合に、印鑑マーク押印管理DB210、及び印鑑マーク複製管理DB211を更新する処理を行う。

【0034】印鑑マーク複製管理プログラムは、社員端末111から印鑑マーク複製要求があった場合に、印鑑マーク押印管理DB210及び印鑑マーク複製管理DB211を登録/更新する。

【0035】また、該印鑑マーク複製管理プログラムは、社員端末111から文書情報確認要求があった場合に、印鑑マーク押印管理DB210、及び印鑑マーク複製管理DB211を参照する処理を行う。

【0036】図3は、社員端末111のハードウェア構成を示す図である。

【0037】本実施形態の社員端末111のハードウェア構成は、図3に示すように、表示装置301と、入力装置302と、通信網インタフェース303と、記憶装置304と、中央処理装置(CPU)305と、一時記憶装置(メモリ)306とが、バス300によって互いに接続されて構成されている。また印影デザインとして従来実社会で使用していた印鑑のデザインを利用する場合

には、イメージスキャナ307を接続して、使用したいデザインをビットマップ等で読み込み、編集できるようにする。

【0038】表示装置301は、社員端末111を使用する社員110にメッセージなどを表示するために用いられるものであり、CRTや液晶ディスプレイなどで構成されている。

【0039】入力装置302は、社員端末111を使用する社員110がデータや命令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【0040】通信網インタフェース303は、通信網120を介して、印鑑マーク管理装置101や社員端末111nなどとデータのやり取りを行うためのインタフェースである。

【0041】記憶装置304は、社員端末111などで使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

【0042】CPU305は、社員端末111を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【0043】メモリ306には、OS306aや、グループウェアシステム等306b、印鑑マーク処理プログラム306c、印鑑マーク情報記憶部306dといった、CPU306が上記の処理をするために必要なプログラムなどが一時的に格納される。

【0044】ここで、OS306aは、社員端末111全体の制御を行うために、ファイル管理やプロセス管

8

理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【0045】グループウェアシステム等306bは、社員端末111が社内外とデータをやり取りし、必要なデータを表示するためのシステムで、データに押印された認証情報を扱うために、印鑑マーク処理プログラム306cとのインタフェースを持つ。なお、この306bの部分は、データをハンドリングするアプリケーションシステムであれば、どのようなものでもよく、特にグループウェアシステムに限定するものではない。また、直接印鑑マーク処理プログラム306cを個別アプリケーションシステムとしてOS上で動かす場合もある。

【0046】印鑑マーク処理プログラム306cは、社員端末111で、印鑑マーク押印処理、印鑑マーク複製処理、印鑑マーク無効化処理、文書認証処理を行うためのプログラムである。印鑑マーク押印処理は、社員110が社員端末111でデータに電子印鑑を押印するための処理で、該社員110に対応する印鑑マークを呼び出す処理、選択された文書特徴量情報と印鑑マークの押印通算Noなどの押印時情報を固有の秘密鍵で暗号化したものを、印鑑マークの特定のブロックに埋め込む処理、及び文書の設定した位置に印鑑マークを押印する処理などを行う。

【0047】印鑑マーク複製処理は、社員110が社員端末111で電子印鑑が押印されたデータ原本からデータの複製(以下、単に複製と称する場合もある)を作成するための処理で、必要なデータを表示し、印鑑マークに添付された公開鍵で埋め込まれた情報を復号化する。そして復号化した情報に対して、文書が改ざんされていないことを確認し、データの有効性及び複製可否を確認の上でデータと印鑑マークを複製し、複製した印鑑マークに対して複製を意味する情報を付加して、固有の秘密鍵で暗号化したものを、印鑑マークの特定のブロックに再び埋め込む処理と公開鍵の添付、及び文書の設定した位置に印鑑マークを押印する処理などを行う。

【0048】印鑑マーク無効化処理は、社員110が社員端末111で電子印鑑が押印されたデータを無効化する処理を行するための処理で、必要なデータを表示し、印鑑マークに添付された公開鍵で、埋め込まれた情報を復号化する。そして、復号化した情報に対して、文書認証情報を確認し、データの原本性を確認の上で、印鑑マークの無効を意味する情報を付加して、固有の秘密鍵で暗号化したものを、印鑑マークの特定ブロックに再び埋め込む処理と公開鍵の添付、及び文書の設定した位置に押印する処理などを行う。

【0049】文書認証処理は、社員110が社員端末111が印鑑マークの内容を確認するためのプログラムである。必要なデータを表示し、印鑑マークに添付された公開鍵で埋め込まれた情報を復号化し、印鑑マークに埋め込まれた情報を元に印鑑マーク管理装置101に確認

(5)

特開2000-76360

9

10

し、原本性と有効性を表示する処理を行う。

【0050】印鑑マーク情報記憶部306dは、社員端末111で、印鑑マーク処理プログラム306cによって、呼び出した印鑑マークや公開鍵を一時的に格納するものである。

【0051】また、公開鍵はあらかじめ社員端末111にFD及びネットワーク上で送付されてもよく、公開鍵の送付方法及び、格納方法は限定しない。

【0052】図4は、印鑑マーク管理DB209のデータ例である。社員ID401、印鑑ID402、氏名403、メールアドレス404、所属・役職他の情報405、印影406などを、一定の表記基準に基づき、表記を統一して格納する。新しい印鑑マークを登録したり、既存の印鑑マークの所属・役職他の情報を変更した際などに、印鑑マーク管理DB209の更新を行う。

【0053】図5は、印鑑マーク押印管理DB210のデータ例である。印鑑ID501、原本通算NO、作成日時、複製可否フラグ504、複製フラグ505、無効フラグ506、ファイル名507、端末ID508、データの特徴情報509などを、一定の表記基準に基づき、表記を統一して格納する。該マーク押印管理DB210には印鑑マークの押印/複製/無効化要求があった際などに、印鑑マーク押印管理DB210などを、一定の表記基準に基づき、表記を統一して格納する。複製可否フラグ504は複製可能カウンタとして複製可能回数を割増することも可能である。無効フラグ506は有効期間として、無効化までの時間をタイマー管理することも可能である。

【0054】該印鑑マーク押印管理DB210のデータは社員端末111の印鑑マーク処理プログラム306cによって、社員端末111で各印鑑マーク認証プログラム306cが管理する秘密鍵によって暗号化して、印鑑マークのエンティティとして埋め込む。データの特徴情報としては、文字データのコードを数値とみなして加算した、いわゆるチェックサムと呼ばれるものや、データ内容の圧縮文などを用いる。埋め込み方法は、例えば、図7の703のように、印影の複製情報を埋め込んだブロック以外の、印影の周辺部分に文書認証情報を埋め込む。

【0055】図6は、印鑑マーク複製管理DB211のデータ例である。印鑑マーク管理装置101で、社員端末111で印鑑マーク複製要求があった場合に、印鑑マーク複製管理プログラム208bが、上位印鑑マーク通算ID601、通算NO602、複製年月日603、複製社員ID504などを、一定の表記基準に基づき、表記を統一して格納する。格納した情報は図5と同様の方法にて、印鑑マークのエンティティとして埋め込む。

【0056】なお、文書認証に必要なデータは、図5、6の例に限らず、ISO9001の認証を取得する際に使用することができる、電子データの記録情報として必

要な情報を満たすものとする。

【0057】図7は、印影及び印鑑マークのイメージ例である。例えば701のような印影に、印鑑マーク複製情報を埋め込む。この時、あらかじめ印影の中を2つ以上のブロックに区分し、各々特定のブロックに印鑑マークの有効性や原本性を意味する情報、及び文書認証情報を埋め込むこととする。例えば、702のように氏名の部分と可視透かしの会社名部分に、印鑑マークの有効性や原本性を意味する情報を埋め込み、703のような印影の周辺部分に文書認証情報を埋め込む、といったブロック区分をし、社員端末111の印鑑マーク認証プログラム306c等で、印鑑マークに埋め込まれた情報を復号化する際には、自動的に対応するブロックから埋め込まれた情報が抽出されるようにする。なお、701では、印影デザイン例として、個人の認め印のデザインを用いたが、日付入りの鑑印や、サイン等のデザイン、複製を表すデザインでもよいし、また社印として用いる際には企業名等でもよく、701の印影デザイン例に限定するものではない。ただし、単なるイメージデザインと異なり、印鑑マークに情報が埋め込まれていると感知されるような、信頼感を与えるマークデザインであることが重要である。

【0058】次に、本実施形態の電子印鑑マーク認証システムの動作について説明する。

【0059】図8は、印鑑マーク処理プログラム306cによって表示される、電子印鑑マーク複製管理システムの初期画面イメージ例である。必要なデジタル文書等を表示する、データ表示エリア801と、印鑑マークの機能ボタンが並び、印鑑マーク機能表示エリア802と、OK、キャンセル、ファイルといった基本機能のボタンが並び、基本機能表示エリア803により、初期画面800が構成される。ただし、初期画面800は、各エリアの配置例であり、この配置に限定するものではない。

【0060】図9は、社員端末111で、印鑑マークを押印したいデータに、文書複製管理情報を埋め込んだ印鑑マークを押印する際の処理フローを説明するための図である。また、図10は、図9の処理フローに対応する処理画面イメージである。この図10と前述の図9を用いて、上記処理フローを説明する。

【0061】まず、社員110が、押印したいデータを、基本機能表示エリア803にあるファイルボタンにより選択し、データ表示エリア801に表示(901)し、印鑑ID501、押印通算No502、作成日時503、複製可否フラグ504、複製フラグ505、無効フラグ506、ファイル名507、端末ID508、データの特徴情報509を印鑑マーク押印管理DB210へ登録する(902)。

【0062】尚、本説明では複製可否フラグ504、複製フラグ505、無効フラグ506の初期値をそれぞれ

(7)

特開2000-76360

11

OK (複製可能)、OFF (原本)、OFF (有効) とするが、社員110及びシステム管理者100によって変更されても良い。

【0063】次に、データより文書特徴量情報を取得して、印鑑マーク押印管理DBの内容とをそれぞれ、社員毎にあらかじめ決められた、各印鑑マーク認証プログラム306cに固有の秘密鍵で暗号化して、印鑑マークに埋め込む(903、904、905)。

【0064】また、その復号化に必要な公開鍵を添付し、押印位置を選択した後、印鑑マーク機能表示エリア802の押印ボタン1004を押下すると、印鑑マーク押印プログラム306cによって、印鑑マークを文書の設定された位置に押印する(906、907、908、909)。なお、印鑑マークに埋め込まれた情報を復号化するために必要な、社員毎固有の公開鍵は、印鑑マークに添付せずにネットワークやFD等で取得する方法でもよい。

【0065】図11は、社員端末111で、マーク印鑑付きのデータ複製処理フローを説明するための図である。また、図12は、図11の処理フローに対応する、複製ボタン1203を押下した際の、処理画面イメージ図である。この図11、12を用いて、上記処理フローを説明する。

【0066】まず、社員110が、複製したい印鑑マーク付きのデータを、基本機能表示エリア803にあるファイルボタンにより選択し、デジタル表示エリア801に表示(1101)する。印鑑マークから印鑑マークに添付された公開鍵を抽出し(1102)、印鑑マークを復号化した後、印鑑マーク押印に関する情報を確認するための印鑑マーク情報と、文書の改ざんを確認するための文書情報を抽出する(1103、1104)。

【0067】次に、該データの特徴量情報を抽出し、1104で取り出した文書情報と比較照合する(1106)。

【0068】比較照合の結果、データが改ざんされていると判断した場合は「このデータは変更されています」等のエラーメッセージを表示する(1107)。

【0069】データが改ざんされていないことを確認したら、印鑑マーク複製管理DBの無効フラグ506よりデータの有効性を確認する。確認の手段として、該印鑑マーク通算No502の複製フラグがOFFであれば、原本と判断し、直ちに該通算Noの無効フラグを確認する。そして、該無効フラグがOFFであれば、有効と判断し、Onであれば無効と判断する。

【0070】また、該印鑑マーク通算No502の複製フラグがOnであれば、複製と判断し、印鑑マーク複製管理DB211より「通算No602の上位印鑑マーク通算No=印鑑マーク押印管理DB210の通算No502」となるデータの無効フラグ506を確認する。

【0071】該データが無効であると判断したら、「こ

12

のデータは無効です」等のエラーメッセージを表示する(1110、1108)。

【0072】該データが有効であることを確認したら、複製可否フラグ504より複製の可否を判断し、複製不可と判断すれば「このデータは複製できません」等のエラーメッセージを表示する(1111、1109)。既記のエラーメッセージの内容は同等の意味を表現するのであれば、変更されてもよく、表現手段も人間の5感に訴えるものであれば何でも良い。

【0073】該データが改ざんされておらず、有効性及び複製可否を確認したら該データは複製可能と判断して、該データと印鑑マーク情報を複製し、複製した印鑑マークの複製フラグ505をOn(複製済み)に設定し、印鑑ID501、通算No502、作成日時503、複製可否フラグ504、複製フラグ505、無効フラグ506、ファイル名507、端末ID508、データの特徴量情報を印鑑マーク押印管理DB210に登録する(1114)。同時に、複製マークに関する情報を、マーク複製管理DB211へ登録する(1115)。登録する情報は、上位印鑑マーク通算No601、通算No602、複製年月日603、複製社員ID604とする。上位印鑑マーク通算Noは該データに押印されている印鑑マークの原本通算No502を取得し、新規に採番された通算Noと階層管理される。

【0074】次に、文書情報と印鑑マーク情報を原本用と複製用のそれぞれ向けに暗号化し、印鑑マークに埋め込む(1116、1117)。

【0075】そして、原本用と複製用の各印鑑マークに復号用の公開鍵を添付して、文書に押印する(1119)。

【0076】上記の処理により、印鑑マーク付きのデータが、原本及び複製の合計2データ作成されることで、印鑑マーク付きデータが複製されたことになる(1202)。

【0077】尚、データへ印鑑マークを押印する位置は1101時と同じ場所であっても、新たに社員110が再指定した位置のいずれであっても良い。また、本説明では複製を1データしか作成しなかったが、複数のデータが一度に複製されても良い。

【0078】図13は、社員端末111で、無効化処理フローを説明するための図である。また、図14は、図13の処理フローに対応する、無効化ボタン1403を押下した際の処理画面イメージ例である。

【0079】まず、社員端末にて無効ボタン1403を押下すると図14の1401となる。尚、選択されたデータ表示から文書情報の比較までの処理は、既記と同じであるが省略する(1301、1302、1303、1304、1305、1306、1307)。

【0080】次に、該データがの原本性を確認するために複製情報の確認を行う。複製情報の確認は該印鑑マ



(8)

特開2000-76360

13

クの複製フラグ505を確認し、該印鑑マークが複製であれば「このデータは複製の為、無効処理できません」等のエラーメッセージを表示する(1309、1308)。

【0081】当印鑑マークが原本であれば、該印鑑マークの印鑑マーク押印管理DB210の無効フラグをOn(無効)にし(1310)、文言情報と印鑑マーク情報を暗号化し印鑑マークに埋め込み、公開鍵を添付して該データに押印する(1311、1312、1313、1314、1402)。

【0082】本説明では、有効なデータを無効化する処理を説明したが、無効なデータを有効化する手段として用いても良い。また、無効フラグ506をOn(無効)にする手段として、印鑑マークに有効期限を持たせて、タイマーで無効フラグがOn(無効)となっても良い。

【0083】無効化したデータに押印する印鑑マークはGUIを変更させて、視覚的に無効化を訴えても良い(1404)。

【0084】図15は社員端末111で、文言情報確認処理フローを説明するための図である。また、図16は、図15の処理フローに対応する、処理画面イメージ例である。

【0085】まず、社員端末111にて文言情報ボタン1603を押下すると、選択されたデータを表示する。該データの表示から文言の特徴量情報と比較照合する処理までは既述と同一であるため省略する(1501、1502、1503、1504、1505、1506、1507)。

【0086】該データが改ざんされていないことを確認したら、印鑑マークより該データが原本または複製であることを確認するために、複製フラグ505の内容を確認する(1509)。次に、該データの有効性を確認する。該データの有効性の確認手段として、該印鑑マーク通算No502の複製フラグがOFFであれば、原本と判断し、直ちに該通算Noの無効フラグを確認する。そして、該無効フラグがOFFであれば、該データは有効と判断し、Onであれば無効と判断する。

【0087】また、該印鑑マーク通算No502の複製フラグがOnであれば、該データは複製と判断し、印鑑マーク複製管理DB211より「通算No602の上位印鑑マーク通算No=印鑑マーク押印管理DB210の通算No502」となるデータの無効フラグ506を確認する。

【0088】該データの有効性が確認できたら、確認結果1604を表示する(1510、1511、1602)。

【0089】以上説明したように、本発明によれば、印影デザインをもつマークをデータに貼付け、このマーク自体に文言情報や印鑑マーク情報を埋め込むことで、一目である程度の情報の確からしさを確認仕組みを提供で

14

きる。また、本発明では、自由に印影デザインを作成できるので、実社会の様々な場面で使用する鑑印、認め印、サイン、社印等と同様のデザインの電子印鑑を、ネットワーク上でも利用できる仕組みを提供することができ。

【0090】

【発明の効果】本発明によれば、印影デザインをもつマークをデータに貼付け、このマーク自体に文言情報や印鑑マーク情報を埋め込むことにより一目である程度の情報の確からしさを確認できる文言管理方式を提供できる。

【図面の簡単な説明】

【図1】本発明の実施形態が適用された電子印鑑複製管理システムの概略構成を示す図

【図2】図1に示す印鑑マーク管理装置のハードウェア構成を示す図

【図3】図1に示す社員端末のハードウェア構成を示す図

【図4】図2に示す印鑑マーク管理DBのデータ例を示す図

【図5】図2に示す印鑑マーク押印管理DBのデータ例を示す図

【図6】図2に示す印鑑マーク複製管理DBのデータ例を示す図

【図7】印鑑マークのイメージ例を示す図

【図8】図1に示す社員端末で、データの文言確認の押印/複製/無効化/確認を行うために必要な情報を、印鑑マークに埋め込む機能と、インターフェイスの初期画面イメージ例を説明するための図

【図9】印鑑マーク押印システムの処理を説明するためのイメージ図

【図10】印鑑マーク押印システムの処理を説明するための図

【図11】印鑑マーク複製システムの処理を説明するためのイメージ図

【図12】印鑑マーク複製システムの処理を説明するための図

【図13】印鑑マーク無効化システムの処理を説明するためのイメージ図

【図14】印鑑マーク無効化システムの処理を説明するための図

【図15】印鑑マーク確認システムの処理を説明するための図

【図16】印鑑マーク確認システムの処理を説明するための図

【符号の簡単な説明】

100：システム管理者

101(1011~101n)：印鑑マーク管理装置

110(1101~110n)：社員

111(1111~111n)：社員端末

(9)

特開2000-76360

15

112: 画面イメージ  
 120 (1201~120n): 通信網  
 200, 300: バス  
 201, 301: 表示装置  
 202, 302: 入力装置  
 203, 303: 通信網インタフェース  
 204: 印鑑マーク管理DBインタフェース  
 205: 印鑑マーク複製管理DBインタフェース  
 206, 304: 記憶装置  
 207, 305: CPU  
 208, 306: メモリ

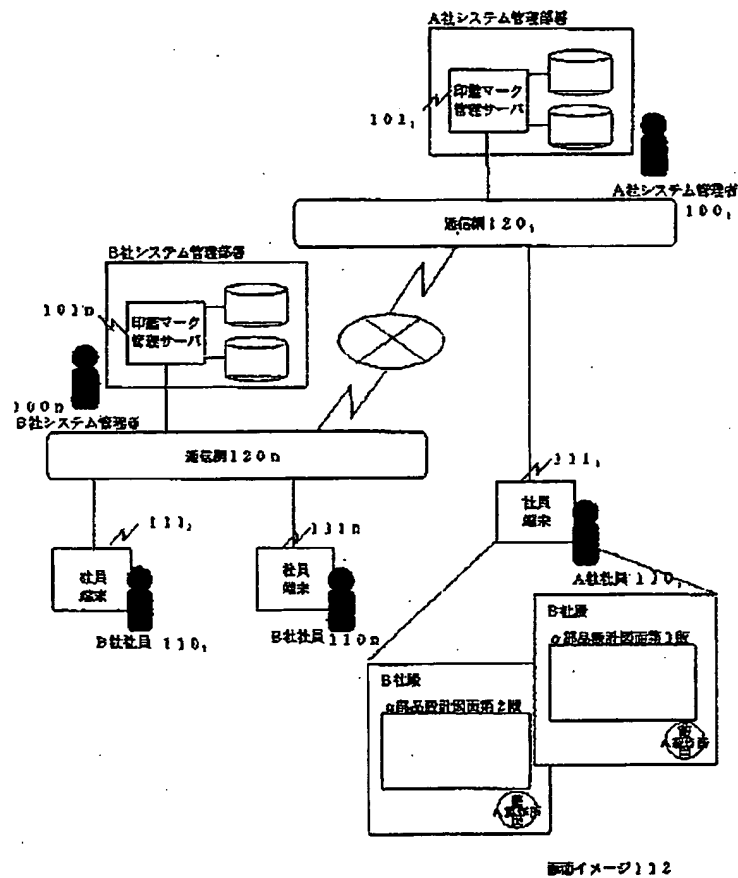
16

\* 209: 印鑑マーク管理DB  
 208a, 306a: オペレーティングシステム  
 208b: 印鑑マーク管理プログラム  
 208c: 印鑑マーク複製管理プログラム  
 210: 印鑑マーク押印管理DB  
 211: 印鑑マーク複製管理DB  
 306b: グループウェアシステム等  
 306c: 印鑑マーク認証プログラム  
 306d: 印鑑マーク情報記憶部  
 307: イメージスキャナ

\*

【図1】

図1

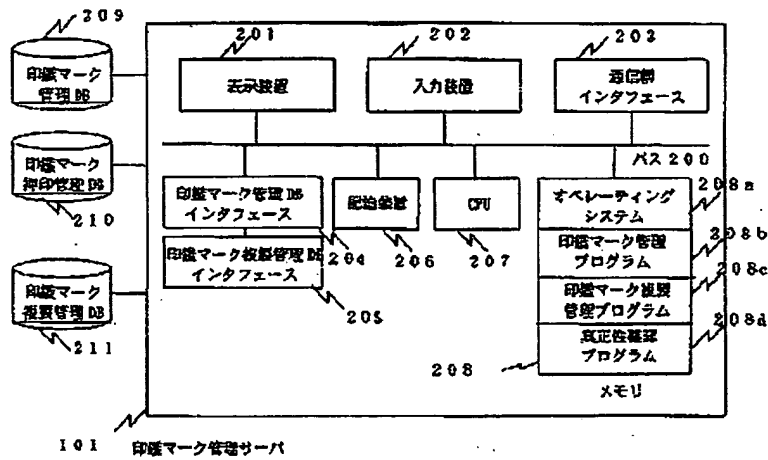


(10)

特開2000-76360

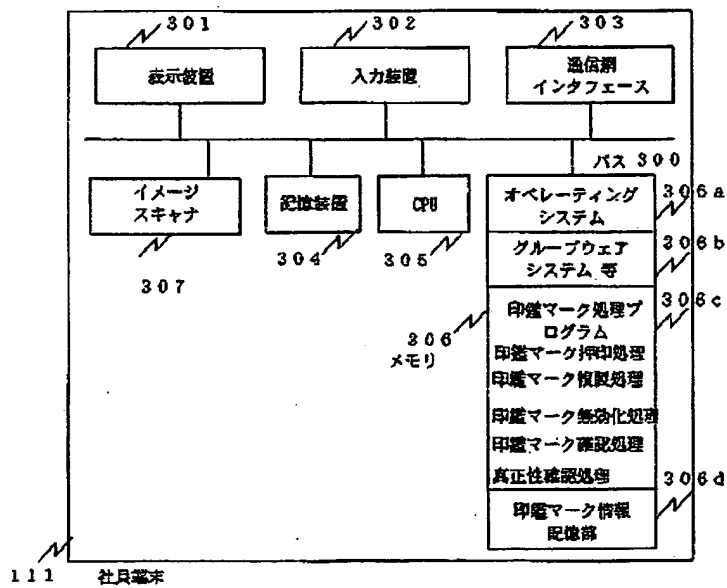
【図2】

図2



【図3】

図3





(11)

特開2000-76360

〔図4〕

図4

社員ID	印鑑ID	氏名	メールアドレス	所属・役職	印影
B001101117	A00111	田川太郎	Aitama@aa.co.jp	〇〇事業部 事業部長	
A035410506	A00114	栗田次郎	Aida@aa.co.jp	〇〇事業部 部長	
B001100482	-	愛野三郎	Aino@aa.co.jp	〇〇事業部 担当	-

〔図5〕

印鑑ID	登録ID	作成日時	複製可否 フラグ	複製 フラグ	複製 フラグ	ファイル名	端末ID	データの複製権限
A00114	029	1998.7.7	OK	OFF	OFF	158.714/91.doc	PC192	*****
A00124	029-01	1998.7.9	OK	OK	OFF	158.249/12.doc	PC193	*****
A00124	029-02	1998.8.1	OK	OK	OFF	158.341/44.doc	PC194	*****

〔図6〕

図6

項目印鑑マ ーク番号	通算NO	複製年月日	複製社員ID
069	089-01	1998.02.01	B001101117
089	089-02	1998.10.01	A035410506

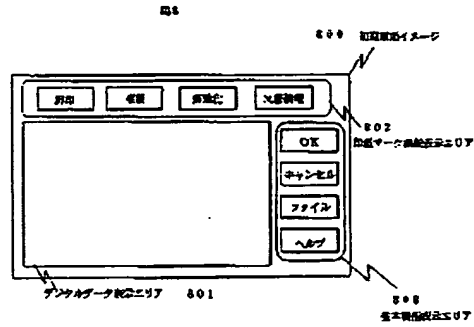
(12)

特開2000-76360

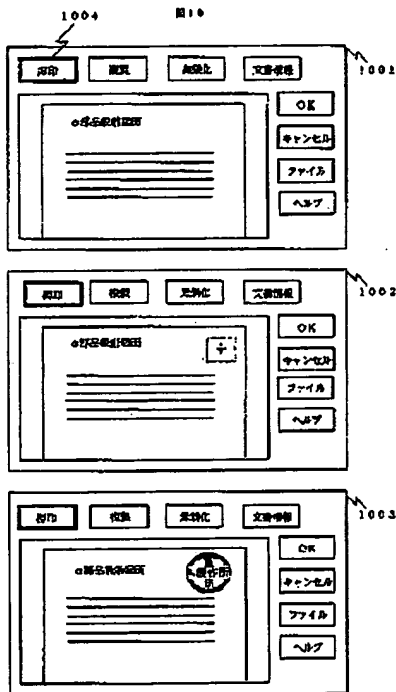
【図7】



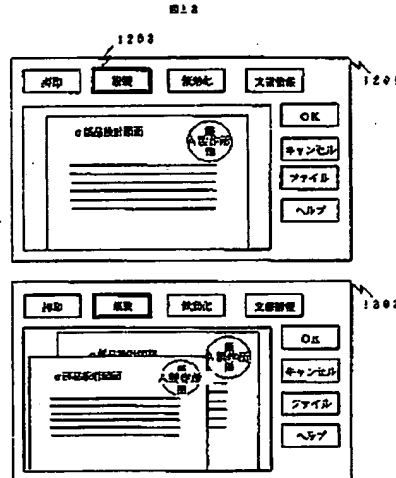
【図8】



【図10】



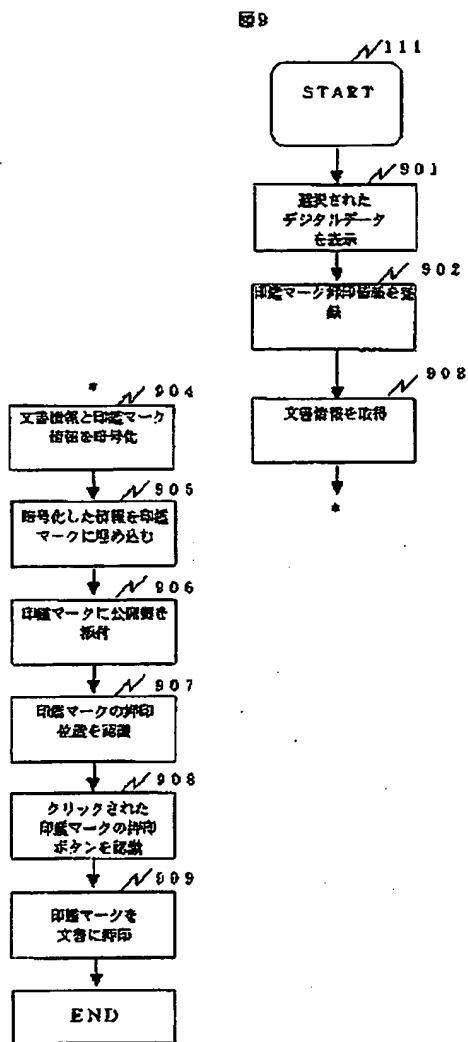
【図12】



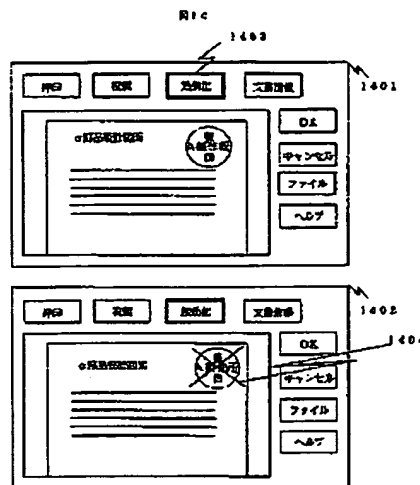
(13)

特開2000-76360

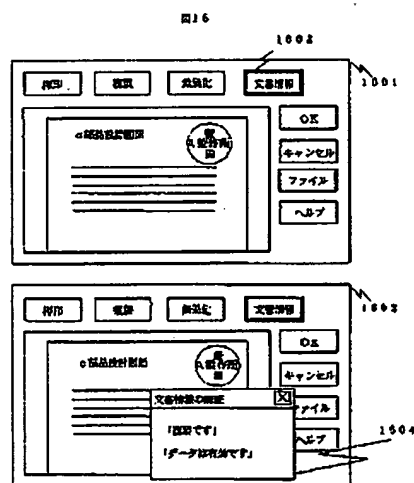
【図9】



【図14】



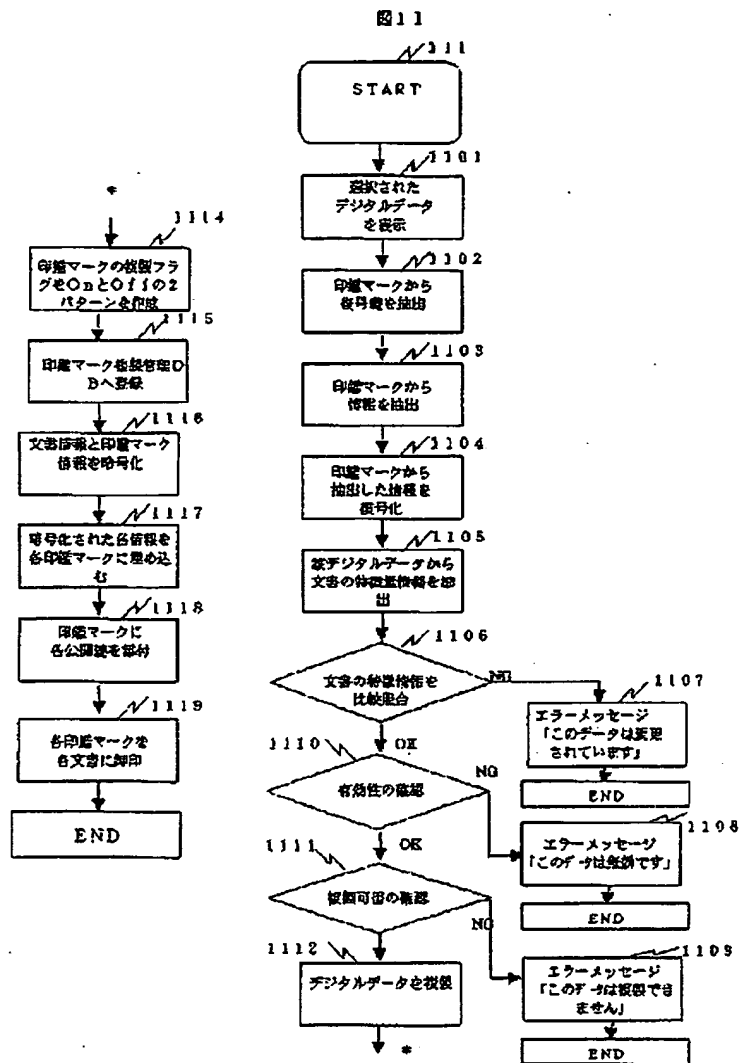
【図16】



(14)

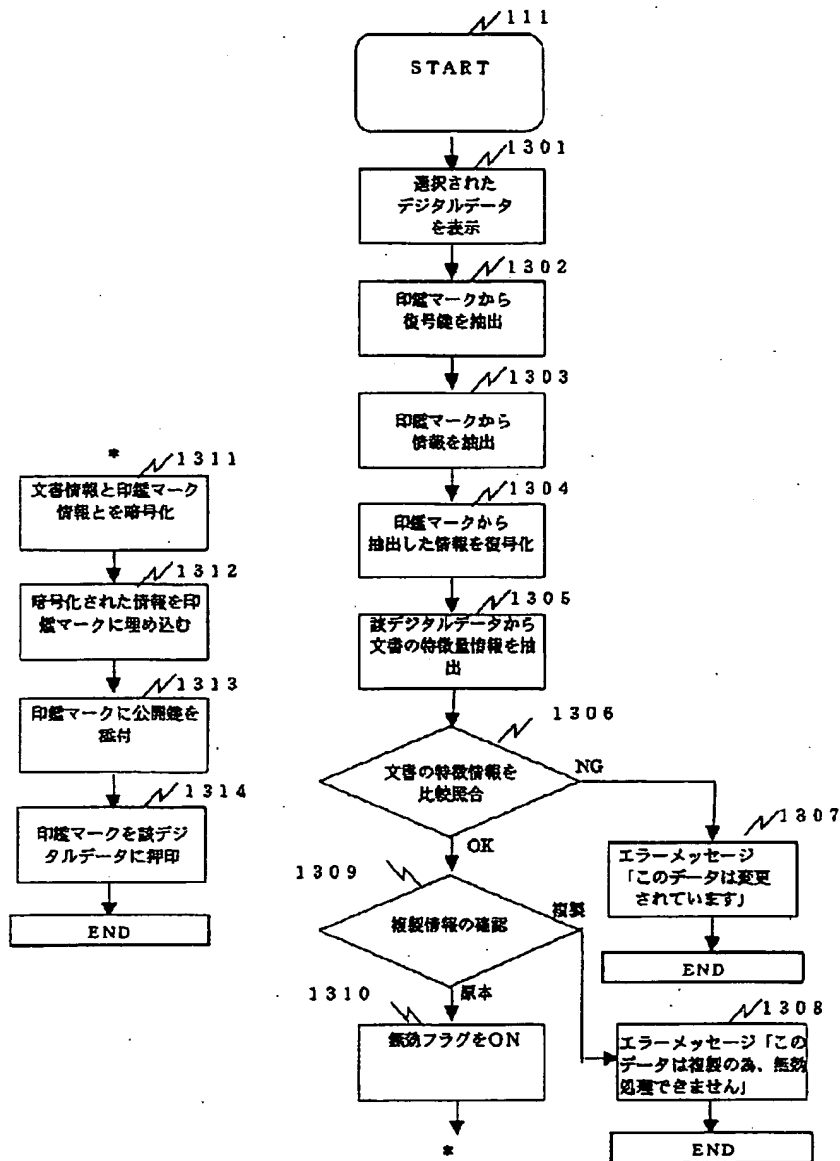
特開2000-76360

【図11】



【図13】

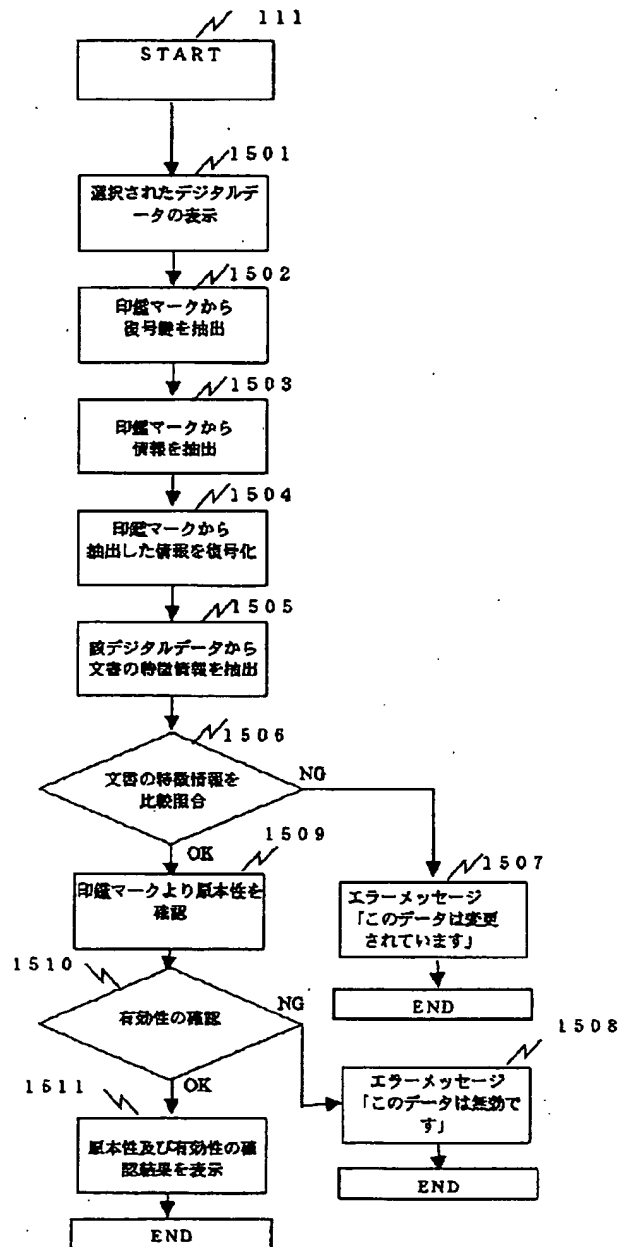
図13





【図15】

図15



フロントページの続き

(51)Int.Cl.

識別記号

F I

キーワード(参考)

G 0 6 F 15/62

4 6 5 P

(72)発明者 永井 康彦

神奈川県川崎市麻生区王禅寺1099番地 株  
式会社日立製作所システム開発研究所内

F ターム(参考) 5B043 AA07 AA10 BA06 BA09 FA02

FA07 GA17 HA02 HA20

5B075 KK43 KK54 ND06 NR06 NR16

PP02 PP03 PP13 PQ02

5C076 AA40

5J104 AA09 LA03 LA05 LA06 MA02

NA02 PA07 PA10

9A001 CZ08 DZ06 DZ07 DZ09 JJ29

JJ66 JJ67 JZ35 LL03

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☒ **OTHER: \_\_\_\_\_**

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**